WEST

Freeform Search

Database: US Patents Full-Text Database

Term:
```
15 and 16
```

Display `10` **Documents in** **Display Format:** `TI`

Generate: ○ Hit List ● Hit Count ○ Image

| Search | Clear | Help | Logout |

Main Menu   Show S Numbers   Edit S Numbers

Search History

DB Name	Query	Hit Count	Set Name
USPT	15 and 16	12	L7
USPT	transaction$ or billing$	62713	L6
USPT	13 same 14	28	L5
USPT	alert$ or announc$ or alarm$ or notif$	101750	L4
USPT	11 same 12	579	L3
USPT	criteria$	84488	L2
USPT	(user adj define$) or customiz$	23904	L1

WEST

Freeform Search

Database: US Patents Full-Text Database

Term: `parker$.in. and 379/$.ccls.`

Display `10` **Documents in Display Format:** `TI`

Generate: ○ Hit List ◉ Hit Count ○ Image

| Search | Clear | Help | Logout |

| Main Menu | Show S Numbers | Edit S Numbers |

Search History

DB Name	Query	Hit Count	Set Name
USPT	parker$.in. and 379/$.ccls.	16	L17
USPT	l11 same l15	39	L16
USPT	l13 same l14	2542	L15
USPT	limit$ or restrict$	1774189	L14
USPT	long adj distance	21911	L13
USPT	l10 and l11	25	L12
USPT	alert$ or notif$ or announc$ or alarm$	101750	L11
USPT	l8 same l9	37	L10
USPT	billing$ or charg$ or transaction$ or balance$	642534	L9
USPT	l6 same l2	591	L8
USPT	l5 and l6	0	L7
USPT	user adj defin$ or (customiz$)	24563	L6
USPT	l3 same l4	12	L5
USPT	telephone$ or phone$	84779	L4
USPT	l1 same l2	56	L3
USPT	criteria	82163	L2
USPT	fraud	2337	L1

WEST

| Help | Logout |

| Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents |

| First Hit | Previous Document | Next Document |

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC |

Document Number 6

Entry 6 of 12   File: USPT   Jun 16, 1998

DOCUMENT-IDENTIFIER: US 5768354 A
TITLE: Fraud evaluation and reporting system and method thereof

ABPL:
Upon receipt of a billing detail record from either an operator or automatic console, a host receiver of the fraud evaluation and reporting system of the instant invention would route a record to either a bad billed number module, a call intercept module or a fraud filter module. Depending on where the record is routed, a determination is made on whether the account number is bad or whether the account number is being used by a fraudulent user. Moreover, calls may be intercepted to determine whether specific predefined thresholds have been exceeded and whether or not subsequent calls are to be processed or denied. Furthermore, by means of the fraud filter processes, various alerts may be generated by applying thresholds relating to different products and division with the account number.

BSPR:
The present invention relates to telecommunications systems and more particularly to a system and a method therefor of monitoring in real time calls into the telecommunications network so as to detect and analyze fraudulent activities, both with respect to the billing account and the originating numbers, by means of a number of different processes.

BSPR:
The instant invention fraud evaluation and reporting (FEAR) system, and the method therefor, provides the operators (analysts or users) of the system the capacity of monitoring call traffic in real time to detect fraudulent activity. The instant invention also allows the users a higher degree of flexibility in establishing the criteria upon which to base decision for taking action to prevent such fraudulent activity. This is accomplished by providing each user the capability to determine what products to monitor and to set limits on the use of such products. Specific numbers and geographic locations can also be defined by the user as suspect; and thresholds can be established by the user on the number of calls of a particular type of product (or service) within specified units of time. When calling activity differs from or exceeds the user defined criteria, alerts are generated by the system.

DEPR:
With reference to FIG. 1, the environment in which the instant invention system operates is provided. As shown, when a subscriber 2 to makes a special service phone call to the telecommunications network, he/she is routed to either a manual operating console 4 where he can converse with an operator or an automatic operations support systems (OSS) console 6. Once the call is set up and the call is routed out of the network to a local switch, a record, otherwise known as a billing detail record (BDR), is made and provided to one of a plurality of RS6000 application based database servers 8. Each of the records is then provided to each of mainframe processors 10, each being an IBM ES/9000 computer. Each of the processors 10 has attached thereto a database BDR store 12 for storing the BDRs. Each processor 10 further has as a part thereof a database distribution system (DDS) and a customer information control system (CICS) by which transactions may be submitted from remote computers to the mainframe processor for processing thereat. Each of the mainframe processors 10 provides redundancy for the other, as each is capable of processing by itself. Thus, each of the mainframe processors 10 is fully functional and has the

same records as the other. Since each of the processors 10 and the components associated therewith are the same, the discussion below is with reference to only one of the processors 10.

DEPR:
Further shown in FIG. 2 are a number of divisions (which are also memory stores or TDQs) communicatively connected to fraud filter module 30. Each of the divisions in actuality may represent a telco located at a specific geographical location, such as the west coast, mid-west or northeast sections of the country--or a company to which a credit or calling card is associated. In other words, each division may have stored in its database a plurality of account or billing numbers which only that division has. Thus, anytime that a call is placed using an account number that is assigned to a given division, the particular products, thresholds and other criteria associated with that given division is used to determine the validity of the account number.

DEPR:
If it is determined that the call is not a special product, the billing number of the record is checked at block 324. If the billing/account number is found to be a valid number, whether the last digit of that billing number is even or odd is next checked per decision block 326. If the billing number of the record is found to be even, the record is routed to the even billing number queue 32. If the billing number is found to be odd, the record is routed to the odd billing record queue 34.

DEPR:
Having thus described the operations of the fraud filter module 30, return to FIG. 3A for the discussion of the billed number module 40 and the originating number module 42. Start with decision block 400. There it can be seen a decision is made on whether the billing number (or account number) is found to be present in a file. If it is not, that bill number is added to the usage table per block 402. Thereafter, a counter which represents the number of times that the billing number has been used is incremented in block 404. The counter is likewise incremented if the bill number is found to be already on file. As shown in FIG. 3B, global thresholds and exception thresholds are next read per block 406. For the embodiment of the instant invention, the global thresholds are assumed to be for domestic calls, international country calls, and target international country calls.

DEPR:
Continuing with the operations of the billed number module 40, the next operation that takes place is a determination of whether there is a bill number exception per decision block 408. A bill number exception occurs if there has been decided previously that a special threshold needs to be provided for a particular account number. For example, assume ordinarily a threshold for a billing number, such as for a domestic call, is 10 for each hour. In other words, if that account number is used to place domestic calls more than 10 times within an hour, an alert signal would be sent. Now assume that it has been determined that that billing number is assigned to a salesman who may very well make more than 10 domestic calls per hour, for example on average the salesman makes 20 calls per hour. Thus, a bill number exception threshold for that bill number may be set at 20 as indicated in block 410. Hence, the 21st call placed within an hour using that particular bill number would be deemed to be over the threshold, and an alert is sent. Of course, if the call usage based on that bill number does not exceed the exception threshold of 20 calls per hour, the operation of the billed number module is terminated for that particular bill number record.
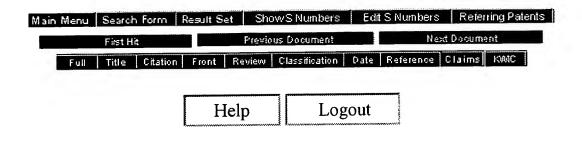
DEPR:
As shown in FIG. 6, the call intercept module begins by reading a record from the intercept queue at block 600. The record must be a BDR and have a billing number and the intercept or fraud flags must be st on the record. These check steps are done in blocks 602 and 604, respectively. Records not meeting this criteria are discarded, while records passing these checks will go through the alert check processing beginning with block 606. Each record reaching the alert check will generate only one alert. The alert generated will be the alert check that matches the flag settings and status conditions on the BDR record. When the alert is triggered, the usage counter will be incremented (block 618) and the alert will be written to the alert table (block 620) which will cause the alert to display on the alert monitor. There are a plurality of alert checks, for example 9, represented by alerts 10, 11, 12, 13 and 14 (represented by blocks 608 to 616 each of which may be checked more than once in order to reach the exemplar 9 checks) that can trigger alerts. Each alert has specific checks and has a special meaning to the fraud analyst. These checks are represented by decision block 608 to 622 and reference the alerts given in the table of FIG. 8.
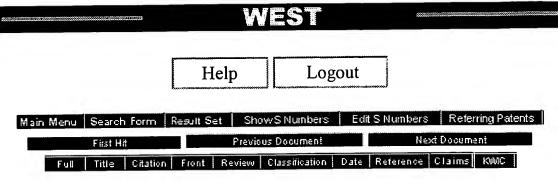
DEPR:

Based on alerts sent to the FEAR monitor, the fraud analyst determine what action they need to take. They can manually go in and set the transfer to fraud flag to "Y" on BNS which will cause the call to a specific billing number to be intercepted. Depending on the alerts generated from the Intercept process, the fraud analyst can then decide what further steps need to be taken to stop this fraudulent caller.

ORPL:
Cellular Business, V9, N12, p. 24(6), Billing Systems: They oren't Just for Billing Anymore, Hank Mishkoff Nov. 1992, ISBN 0741-6520.

Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents

First Hit	Previous Document	Next Document

Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Help	Logout

WEST

Help	Logout

Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents

First Hit	Previous Document	Next Document

Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Document Number 9

Entry 9 of 12   File: USPT   Jan 7, 1997

DOCUMENT-IDENTIFIER: US 5592375 A
TITLE: Computer-assisted system for interactively brokering goods or services between buyers and sellers

ABPL:
A computer-implemented system for brokering transactions between sellers and a buyer of goods or services, including a database, a seller interface, and a buyer's interface. The database contains information, including multimedia information, descriptive of respective ones of the goods or services. The seller interface enables the sellers to interactively enter information, including multimedia information, into the database. The buyer's interface provides a knowledge-based interactive protocol, enabling the buyer to select and review the descriptive information from the database, and makes perceptible the multimedia information in response to an interactive buyer request.

BSPR:
The invention provides a computer-based system to facilitate any transaction where review of diverse information is a part of the buyer's decision-making process. It allows information in a number of forms to be submitted by the seller, compiled in a database and reviewed by the buyer with the assistance of an interactive, expert system based, networked computer system.

BSPR:
In general, the invention features a computer-implemented system for brokering transactions between sellers and a buyer of goods or services, the system including a database, a Seller's Interface, and a Buyer's Interface. The database contains information, including multimedia information, descriptive of respective ones of the goods or services. The Seller's Interface enables the sellers to interactively enter information, including multimedia information, into the database. The Buyer's Interface provides a knowledge-based interactive protocol, enabling the buyer to select and review the descriptive information from the database, and makes perceptible the multimedia information in response to an interactive buyer request.

BSPR:
Preferred embodiments of the invention may include the following features. The Seller's Interface enforces entry by the seller of at least a predefined minimum set of information about each of the goods. The descriptive information includes profile vectors of optional information. The information of each profile vector is associated with other information in the profile vector but is independent of information of the other profile vectors for the same good or service. The Buyer's Interface records actions of the buyer in an action log for later use, and a report generator extracts information from the action log to provide feedback information to the buyers and/or sellers. At least one of the Seller's Interface and the Buyer's Interface has two modes, a first mode having relatively slower interactivity for use with a low-bandwidth communications channel, and a second mode having relatively faster interactivity for use with a high-bandwidth channel. The system may have automatic notification elements for notifying the buyer of descriptive information newly-entered into the database that matches selection criteria previously specified by the buyer. The Buyer's Interface may also have, two modes of operation, a first mode for specifying selection criteria for selecting descriptive information from the database, and a second mode allowing detailed study of the selected descriptive information. The knowledge-based protocol includes an approximate-comparison system, for presenting to the buyer, goods or services that approximately match selection criteria entered

into the Buyer's Interface. In one approximate-comparison system, the buyer is presented those goods or services that meet <u>user-defined</u> required <u>criteria,</u> and closely meet <u>user-defined desired criteria</u>.

BSPR:
This system can be used in a variety of <u>transaction</u> applications which include, but are not limited to:
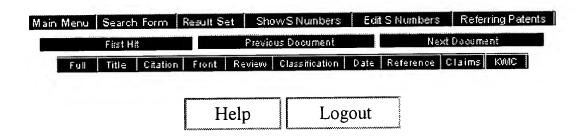
DEPR:
The Action Log also is the basis for <u>billing</u> for system services. In general, both buyers and sellers would pay a subscription fee for access to the system. Charges could also be made for connect time, communications costs, database storage and other system services. Each match that results in a completed <u>transaction</u> could also incur a charge to the buyer or seller depending upon the application.

DEPR:
There are a large number of additional applications that involve similar purchasing decisions, and to which the system is applicable. Applications that are <u>transaction-oriented</u> and require matching of criteria as a part of the decision making process can use a system that identifies and mechanizes a core set of criteria, augments it with multimedia information and automates the process of collection and presentation of the information.

DEPR:
Consumer or commercial product selection involves use of a wide area network coupled with a broad band video delivery "highway". As the system is designed to be network-independent, it can provide the coupling of structured information and multimedia presentation to broker <u>transactions</u> of consumer goods and services. Automobiles, travel, white goods, and fashions are further examples of applications that the system can address.

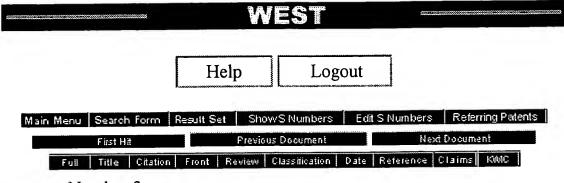| Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents
First Hit		Previous Document		Next Document	

Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Help   Logout

WEST

Freeform Search

Database: US Patents Full-Text Database ▼

Term:
```
17 same 19
```

Display `10` **Documents in Display Format:** `TI`

Generate: ○ Hit List ⊙ Hit Count ○ Image

| Search | Clear | Help | Logout |

| Main Menu | Show S Numbers | Edit S Numbers |

Search History

DB Name	Query	Hit Count	Set Name
USPT	17 same 19	6	L10
USPT	telephone$ or phone$	84779	L9
USPT	(call$)	568917	L8
USPT	13 same 16	128	L7
USPT	(user adj (define$ or specifi$ or select$)) or customiz$	42477	L6
USPT	13 same 14	6	L5
USPT	(long adj distance) with call$	1636	L4
USPT	11 same 12	21460	L3
USPT	(exceed$ or met) with (threshold$ or limit$ or criteria$)	107728	L2
USPT	(alert$ or notif$ or announc$ or indicat$)	1381200	L1

WEST

| Help | Logout |

| Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents |

| First Hit | Previous Document | Next Document |

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC |

Document Number 3

Entry 3 of 6   File: USPT   Feb 23, 1999

DOCUMENT-IDENTIFIER: US 5875236 A
TITLE: Call handling method for credit and fraud management

ABPL:
Prior to completing a telephone call, a database is accessed within a telecommunications network to determine whether the call should be completed. The billing number to which the call is to be charged is compared to a customer record assigned to the billing number and stored in the database. The customer record is checked against a treatment category code which combines geographic call restrictions and thresholding. A call may be identified as potentially fraudulent and blocked if the customer record associated with the billing number indicates that the account is in arrears. In addition, at predetermined intervals during the progress of the call and at the end of each allowed call to be charged to that billing number, the time and/or cost of each call is estimated and added to the total stored in a user-defined threshold counter in the database. When the total stored in the counter exceeds a predetermined threshold limit, a potentially fraudulent call is identified. In this manner, call authorization is performed on a per call basis to prevent fraudulent telephone calls.

DEPR:
For each user defined threshold counter, the customer's assigned treatment category also defines at least one threshold level to alert the NAI [40] and the IXC when the particular customer has exceeded the user defined threshold. Preferably, more than one threshold limit may be defined for each threshold counter. Therefore, irrespective of whether the NAI [40] stores usage time (minutes) or the estimated cost of the call (dollars and cents) in the threshold counters, the NAI [40] compares the total (minutes or dollars) to the predefined threshold limits for the particular threshold counter (step S21). When a threshold limit is exceeded (step 122), the NAI [40] identifies the customer as a potentially fraudulent caller (step S23) and takes certain precautionary/investigatory actions, such as denial of the call, interrupting the call in progress, or redirecting the call to an appropriate work center of the IXC (step S24). As such, the NAI [40] may monitor a specific customer's calling patterns on a real time basis to determine if the customer's telephone usage is indicative of potentially fraudulent activity.
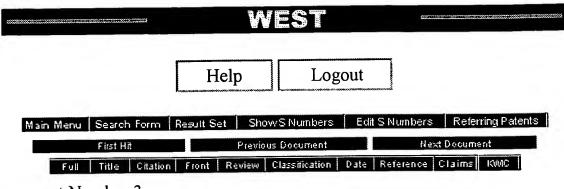
WEST

Freeform Search

Database: US Patents Full-Text Database ▼

Term: 16 and 14

Display 10 **Documents in Display Format:** TI

Generate: ○ Hit List ⦿ Hit Count ○ Image

| Search | Clear | Help | Logout |

Main Menu   Show S Numbers   Edit S Numbers

Search History

DB Name	Query	Hit Count	Set Name
USPT	16 and 14	12	L7
USPT	notif$ or alert$ or indicat$	1379919	L6
USPT	11 and 14	1	L5
USPT	12 same 13	13	L4
USPT	(exceed$ or met or meet$) with (threshold$ or limit$ or balance$ or amount$)	160352	L3
USPT	cdr or (call adj detail adj record$)	1695	L2
USPT	internet	6738	L1

WEST

| Help | | Logout |

| Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents |

| First Hit | Previous Document | Next Document |

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC |

Document Number 3

Entry 3 of 12   File: USPT   Sep 8, 1998

DOCUMENT-IDENTIFIER: US 5805686 A
TITLE: Telephone fraud detection system

ABPL:
A fraud detection system is disclosed for telephone PBX calls. The system includes a fraud data server for buffering the call detail records relating to inbound 800 number calls and outbound international calls. A threshold manager is connected at its input to an output of the fraud data server for detecting numerical counts exceeding preselected threshold values, in predetermined fields of the call detail records, and generates an alarm. The output of the threshold manager is connected to an input of the fraud data server for buffering the alarm incident to respective call detail records. A computer workstation is connected to the fraud data server for receiving packets of call detail records relating to alarm data, in a filtered preselected format. The workstation includes a monitor for displaying the alarm data on a graphical interface.

BSPR:
At the present time, fraud analysis of PBX use is typically done by manually reviewing call data records, after an initial data sorting, to detect patterns indicative of fraud. However, as will be appreciated, this is a laborious and time-consuming process which results in long delays between the actual occurrence of fraud and the manual review and detection thereof.

BSPR:
A threshold is a number which, when exceeded, generates an alarm in MCI Detect indicating possible fraud. For example, if a customer indicates that it should receive no more than 1000 calls to its 800 number on any given business day, then the number "1000" is a threshold, and the 1001st call will generate an alarm. Thresholds may be specified for the time of day and/or the day of the week. Furthermore, a threshold may be applied to each category for which MCI Detect keeps counts, including the number of short-duration calls, long-duration calls, and cumulative minutes.

BSPR:
As described previously, risk factors and suspect numbers help to determine the likelihood of fraud based on the assumption that some types of calls more clearly indicate fraud than others. For example, a call from a high-risk dialing area may be assigned a weight of 3.0. Each time such a call is recorded, relevant counts are multiplied by a factor of 3 and thresholds are exceeded more quickly. The detection of a suspect number immediately triggers an alarm in MCI Detect. It is not necessary to apply weights to these numbers.

BSPR:
Each alarm is available to an MCI fraud analyst via an MCI Detect Workstation. The workstation is a PC with access to a Fraud Data Server and retrieves the next available alarm of the highest priority. The analyst investigates the alarm data and, if fraud is suspected, notifies the customer and suggests appropriate actions to stop the fraud.

BSPV:
Numerous short duration calls which may indicate that hackers are attempting entry.

BSPV:
Excessively long calls which may indicate that hackers are using inbound trunks to make outbound calls;

BSPV:
MCI Detect's timely detection and notification of 15 minutes or less.

BSPV:
Risk factors are applied to NPA-NXXs, information digits, and specific countries, which minimizes false alarms and also provides early notification of abnormal calling patterns.

BSPV:
Customers will have the option of specifying any of the following media for alarm notification: telephone, MCI Mail.TM., fax, pager Integrated Network Management Services (INMS), or Integrated Customer Workstation (ICW).

DRPR:
FIG. 2 is a block diagram of the system architecture for the present invention, indicating greater detail than that shown in FIG. 1.

DEPR:
The following will describe the system operation as indicated in FIGS. 2 and 3.

DEPR:
Referring to FIG. 2, the architecture of the present invention is shown in greater detail. The MCI network 4 generates call detail records (CDRs) which are input to an IBM-based computer system, indicated in block 6 as a T2000 (Traffic 2000). The system stores CDRs generated by the network 4. The T2000 system conventionally processes billing data, as indicated by reference numeral 8. The CDRs and billing data are retained in the T2000 for a period of time normally required to conduct fraud analysis. Typically, this would be for a period of 24 hours. The components 4, 6 and 8, employed by MCI Detect 10, constitute prior art.

DEPR:
With continued reference to FIG. 1, the output of the T2000 can provide call records including CDRs and billing data to the input of the MCI Detect system 10, and more particularly to a fraud data server (FDS) 16. The server is of conventional design and includes a buffer for recently retrieved call records which have been obtained from the T2000. The FDS provides call records to a threshold manager (TM) which processes the call records by reviewing the fields thereof and comparing these fields with established thresholds. When thresholds are exceeded, they indicate the possible occurrence of fraud.

DEPR:
The workstation 12 is preferably a PC workstation operating with an OS/2 operating system. FIG. 3 indicates the workstation 12 in greater detail. The workstation communicates bidirectionally with the FDS 16, the latter keeping track of updated alarm conditions fed back from the TM 14. The FDS produces alarm summaries from the alarm data fed back from the TM 14. The communications manager 18 provides alarm summary information packets to other objects of the workstation. In FIG. 3, the presence of recent actual alarm summaries, tabulatable on a priority basis, is indicated by object 22. Call detail records, as indicated by workstation object 24, are presented in graphical interface format to an analyst who can change the status of a particular alarm situation, as well as various status conditions. These changes are communicated to the FDS 16 by virtue of a communications path back through the alarm summary object 22 and the communications manager 18. From time to time, it may be necessary to change the thresholds of the TM 14. Threshold conditions vary for different accounts, according to preselected sets of parameters, referred to plan management, and indicated in FIG. 3 by object 20. The parameters are shown in various examples in FIGS. 5 and 6.

DEPR:
The MCI Detect Threshold Manager provides real-time threshold analysis (that is, it continuously monitors for plan thresholds that have been exceeded) using algorithms (for example, number of short-duration inbound 800 calls). Examples are indicated in FIGS. 5 and 6. It receives call detail records from the Fraud Data Server 16 and returns alarms which may be retrieved and examined using an MCI Detect workstation. The threshold manager resides on an IBM RS/6000 computer running the AIX operation system.

DEPR:
The TM then applies a risk factor 924 to the call data. A risk factor represents a co-efficient that is entered by the customer to indicate increased risk associated with a particular NPA-NXX, country, calling area, or info digits. If none is entered, the default risk factor is 1. The TM calculates risk-adjusted counts 926 by multiplying the actual counts by the risk factor. For example, if the customer enters a risk factor of 3 for calls received from NPA-NXX 202-887, and a call record is received for a short-duration 800 call from the ANI 202-887-nnnn, the short-duration count of the monitoring plan is increased by 3.

CLPV:
a threshold manager connected to an output of the fraud data server for keeping numerical counts of call data in predetermined fields of the call detail records, multiplying the numerical counts by predetermined risk factors to obtain risk-adjusted counts, detecting risk adjusted counts exceeding preselected threshold values, and generating an alarm in response thereto;

CLPV:
detecting risk adjusted counts exceeding preselected threshold values, in predetermined fields of the call detail records;

CLPV:
a threshold manager connected to an output of the fraud data server for accepting the call detail records from the parsing means and detecting numerical counts exceeding preselected threshold values, in predetermined fields of the call detail records, and generating an alarm in response thereto;

CLPV:
accepting the parsed call detail records for detecting numerical counts exceeding preselected threshold values, in predetermined fields of the call detail records;

CLPV:
a threshold manager connected to an output of the fraud data server for detecting numerical counts exceeding preselected threshold values, in predetermined fields of the call detail records, generating an alarm in response thereto and prioritizing the alarm according to how many times the threshold has been exceeded;

CLPV:
detecting numerical counts exceeding preselected threshold values, in predetermined fields of the call detail records;

CLPV:
a threshold manager connected to an output of the fraud data server for keeping numerical counts of call data in predetermined fields of the call detail records, multiplying the numerical counts by predetermined risk factors to obtain risk-adjusted counts, detecting risk adjusted counts exceeding preselected threshold values, and generating an alarm in response thereto and prioritizing the alarm according to how many times the threshold has been exceeded;

CLPV:
detecting risk adjusted counts exceeding preselected threshold values, in predetermined fields of the call detail records;

Help   Logout